REMARKS

Applicants have carefully reviewed the Office Action dated May 16, 2005, the cited references, and the Examiner's reasons for rejection of the claims. Applicants respectfully submit that, based on this Response, this application is in condition for full allowance, and Applicants respectfully request such allowance.

Drawings

In the Office Action mailed May 16, 2005, the Examiner objected to the drawings, requesting corrected formal drawings. Formal drawings labeled "replacement sheets" are enclosed with this response.

Response to Rejections under Section 103

In the Office Action dated May 16, 2005, the Examiner rejected claims 1-24 under 35 U.S.C. Section 103(a) as being unpatentable over Van Dyke (U.S. Patent No. 5,708,812) further in view of Mehring (U.S. Patent No. 6,609,115). The Examiner will recall that the present invention as generally directed to a method for migrating (as in claim 1) and populating user identification and password data (as in claims 16 and 22) from a source user authenticator to a target user authenticator. One of the novel aspects of the invention as claimed in clams 1, 16, and 22 is the method of logging in the user if the user logs into the target user authenticator and the target user authenticator does not have the user's password associated with the user's identification. In this instance, claims 1, 16, and 22 provide for submitting the received identification and password to the source user authenticator. The source user authenticator is monitored for an approval response and upon receipt of an approval response from the source user authenticator, the target database (associated with the target user authenticator) is populated with the user's password and the password is associated with the user's identification. The target user authenticator then authenticates the user identification and password.

In rejecting independent claims 1, 16, and 22, the Examiner states that Van Dyke does not teach certain aspects, including that the if the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator. In support of the rejection, the Examiner points to Mehring.

Applicant has carefully reviewed the references and text cited by the Examiner. The cited

text in Mehring (col. 10, lines 49-67, col. 11, lines 1-10) fails to disclose Applicants' claimed invention including where the target user authenticator does not have the password associated with the user identification to submit the request to the source user authenticator. Mehring discloses a remote user logging into a web server and the web server validating the user via a policy server. Once authenticated the user is issued an authenticity tag by the policy server that is stored on the remote user system and the web server. Future requests by remote system user to web servers are expedited by using the authenticity tag.

The Mehring disclosure fails to teach, disclose, or suggest the elements of Claims 1, 16, and 22 that if the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator. Mehring's web server and policy server are not analogous to Applicants' target user authenticator and source authenticator, between which authentication data is migration. Also, there is only one route suggested in the Mehring disclosure, while Applicants' claim provides for this novel authentication approach if the target datastore does not include a password associated with the identification. For this reason, Applicants request the Examiner to withdraw the rejection of claims 1, 16, and 22, and the dependent claims that depend therefrom pass these claims to issue.

The Examiner then states that Van Dyke discloses the aspects of Applicants' claims of monitoring the source user authenticator for a response. The cited text of Van Dyke (col. 17, lines 1-29) discloses that a user may log into the Source Domain via the Target Domain by specifying the user's Source Domain account and then user obtains a security identifier that uniquely identifies a user within a network domain, in this case the user obtains both a Source and Target Domain security identifiers. The cited text contains other variations, but the user still user obtains both a Source and Target Domain security identifiers

Applicants submit that Van Dyke fails to teach any monitoring of the Source or Target Domains for an approval response. Furthermore, Applicants submit that Van Dyke, either alone or in combination with Mehring, fails to teach the context of Claims 1, 16, and 22 that if the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator, and monitor the source authenticator for an approval response. Therefore, Applicants request the Examiner to

withdraw the rejection of these claims and pass same to issue.

The Examiner states the Van Dyke fails to teach that on receipt of an approval response from the source user authenticator to populate the target user authenticator with the received password and to associate the password with the user's identification. The Examiner states that it would have been obvious to one skilled in the art on receipt of an approval response from the source user authenticator to populate the target datastore with the received password and to associate the received password with the corresponding identification since, according to the Examiner, it is well known in the art to facilitate the complete transfer of data when data is found missing from the original source, it is restored by the data from the original source.

Applicants respectfully submit that a prima facie case of obviousness under 35 U.S.C. Section 103 is improper unless each and every element of Applicants' invention is either disclosed, taught, or suggested by the cited references. Applicants respectfully submit that the obviousness rejection is improper since the Examiner agrees that the cited references fail to provide any teaching or suggestion that on receipt of an approval response from the source user authenticator to populate the target user authenticator with the received password and to associate the password with the user's identification. Applicants' novel invention, as claimed in claims 1, 16, and 22 includes if the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator, and monitor the source authenticator for an approval response. Upon receipt of an approval response from the source user authenticator, the target database is populated with the user's password and the password is associated with the user's identification. The cited references, either alone or in combination, fail to teach, disclose, or suggest Applicants' invention as claimed in claims 1, 16, and 22. For these reasons, Applicants respectfully request the Examiner to withdraw the rejection of these claims, and the dependent claims that depend therefrom, and pass these claims to issue.

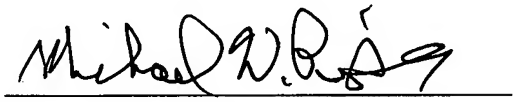
Independent claim 19, and dependent claims 20 and 21 which depend therefrom, includes some of the novel aspects discussed above and which for the reasons stated above are not taught, disclosed or suggested by the cited references. Claim 19 also includes that if the target datastore does include a password associated with the identification, then: authenticating the identification and password using the target user using the target user authenticator. The Examiner only cites

to Van Dyke (col. 7, lines 15-20) in the rejection without any remarks. However, Applicants have carefully reviewed the reference and the cited text which states that "each user or service account in a domain is stored with a password and corresponding unique account identification with the Source Domain which is used by the domain controller to access security context corresponding to a user or service." The cited text states that each user has a stored password and user identification. Claim 19 specifically states that target datastore does not include a password. For this reasons, Applicants fail to find any teaching or disclosure in the cited reference as claimed in claim 19 that if the target datastore does include a password associated with the identification, then: authenticating the identification and password using the target user using the target user authenticator. Therefore, Applicants request that the Examiner withdraw the rejection of Claim 19 and pass claims 19, and dependent claims 20 and 21, to issue.

Conclusion

Applicants respectfully submit that the present application is in condition for full allowance for the reasons stated above, and Applicants respectfully request such allowance. If the Examiner has any questions or comments or feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. This correspondence is intended to be a complete response to the Office Action dated May 16, 2005. The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 21-0765, Sprint.

Respectfully submitted,



Date: August 16, 2005

Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANT

CONLEY ROSE, P.C.
5700 Granite Parkway, Suite 330
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)